Suricata - Feature #2996
Extend decode events and rules
05/29/2019 08:05 AM - Andreas Herz

Status: Assigned
Priority: Normal
Assignee: Andreas Herz
Category: 
Target version: TBD
Effort: medium
Difficulty: low

Description
We already have several decode events and rules but there are still some missing. For example we have the stream.reassembly_overlap_different_data stream event and rule for that but we're missing the one for stream.reassembly_overlap where we have just the tcp.overlap counter.

History
#1 - 05/30/2019 05:00 AM - Victor Julien
- Tracker changed from Optimization to Feature
- Status changed from Assigned to New
- Assignee changed from OISF Dev to Community Ticket

#2 - 06/30/2019 07:57 PM - Shivani Bhardwaj
Hey Andreas!
Could you please link a document where I can match what else are we missing? I'm just browsing through the code and finding these values. I do not see REASSEMBLY_OVERLAP in any enums so that's one. Also, if this issue is concerned with stream.reassembly_overlap only, let me know that as well.

#3 - 06/30/2019 08:41 PM - Andreas Herz
I also found this just by "accident" as I was looking into some overlap infos. I can start a list, maybe it's not very long. Did you find any others?

#4 - 07/01/2019 08:39 PM - Andreas Herz
At least those are missing:
- tcp.reassembly_gap
- tcp.overlap
- tcp.insert_data_normal_fail
- tcp.insert_data_overlap_fail
- tcp.insert_list_fail

I guess this might be a bigger task to collect all possible events.

#5 - 07/03/2019 09:12 AM - Victor Julien
For every event there should be a rule in the rules/*-events.rules files.

#6 - 07/05/2019 09:52 PM - Andreas Herz
For those implemented yes, but some are missing or is there a specific reason why there is a StreamTcpSetEvent(p, STREAM_REASSEMBLY_OVERLAP_DIFFERENT_DATA); but no StreamTcpSetEvent(p, STREAM_REASSEMBLY_OVERLAP); or StreamTcpSetEvent(p, STREAM_REASSEMBLY_LIST_FAIL);?

But tcp.reassembly_gap is covered by tcp.reassembly_gap so that's not missing.

If I look into StreamTcpThreadInit where we register the counter I see also some where it's quite obvious that we don't want to trigger an event for every StatsIncr of those.

I guess there is no easy way to determine which ones are missing beside the overlap and insert fails. It might be enough to cover those which we found and add even more if someone spots a missing one that might be handy for debugging.

That's why I stumbled upon that, while I wanted to dig into why there are sometimes high tcp.overlap values and with a rule it would help to narrow it
down where they appear.

Thoughts?

#7 - 09/24/2019 08:40 PM - Andreas Herz
   - Assignee changed from Community Ticket to Andreas Herz

#8 - 09/26/2019 08:31 AM - Victor Julien
   Lets just add the missing ones, but commented out by default.

#9 - 10/21/2019 08:35 PM - Andreas Herz
   - Status changed from New to Assigned